



Official incident report

Event ID: 78

Rule Name: SOC139 - Meterpreter or Empire Activity

Made By

LinkedIn: Engineer.Ahmed Mansour

Link: <https://www.linkedin.com/in/ahmed-mansour-5631b5323/>

Github link: <https://github.com/AhmedMansour93>

Table of contents

Official incident report	1
Event ID: 78	1
Rule Name: SOC139 - Meterpreter or Empire Activity	1
Table of contents	2
Event Details	3
Network Information Details	4
Analysis	5
Log management	5
Security Email	6
Detection	7
Threat intelligence	7
Endpoint Security	10
Conclusion	13

Event Details

Event ID:

78

Event Date and Time:

Mar, 15, 2021, 02:15 PM

Rule:

SOC139 - Meterpreter or Empire Activity

Level:

Security Analyst

Hostname:

Alex - HP

File Name:

cobaltstrike_shellcode.exe

File Hash:

24d99ba5654cdf31141c66fd9417b7e0

File Size:

219.00 Kb

Device Action:

Allowed

Network Information Details

Destination IP Address:

13.107.4.50 external

Source IP Address:

172.16.17.55 internal

Destination IP Address: • 13.107.4.50 (External)

- This is a public IP address, indicating traffic from outside your organization's internal network. The destination IP suggests that the internal device is attempting to communicate with an external service or server. Depending on the context, this connection could represent legitimate access or a potential security concern.

Source IP Address: • 172.16.17.55 (Internal)

- This IP address is part of your organization's private IP range (172.16.0.0 to 172.31.255.255), indicating it belongs to a device within your local network. The internal device with this address is initiating the communication, which means the activity is originating from within your environment.

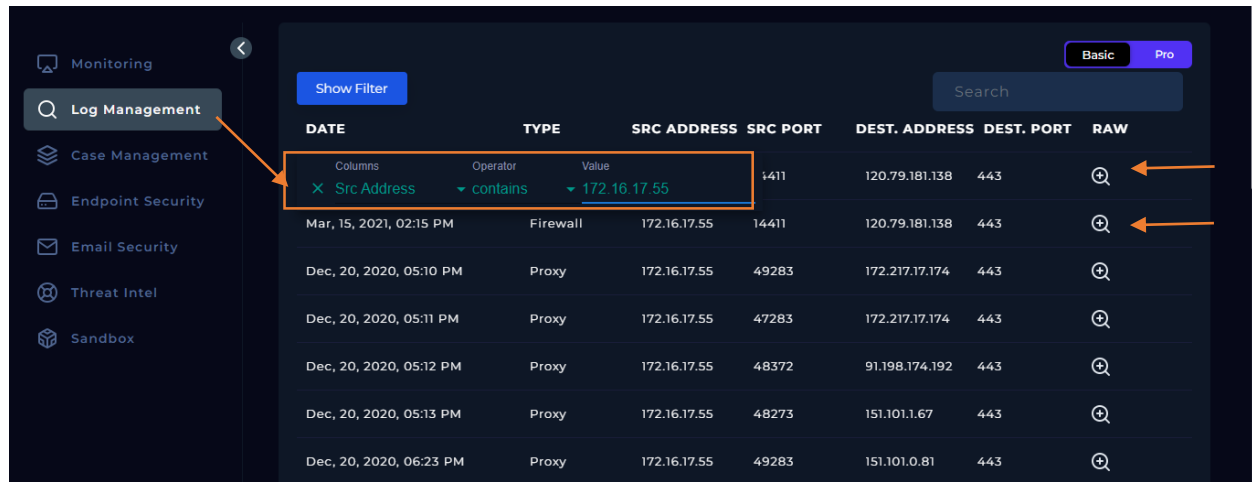
- **The attack is external**

Analysis:

Log Management

We'll proceed by entering the Source IP address and reviewing the results. Based on the time and date of the attack.

Please refer to the attached image for further details regarding the attack.



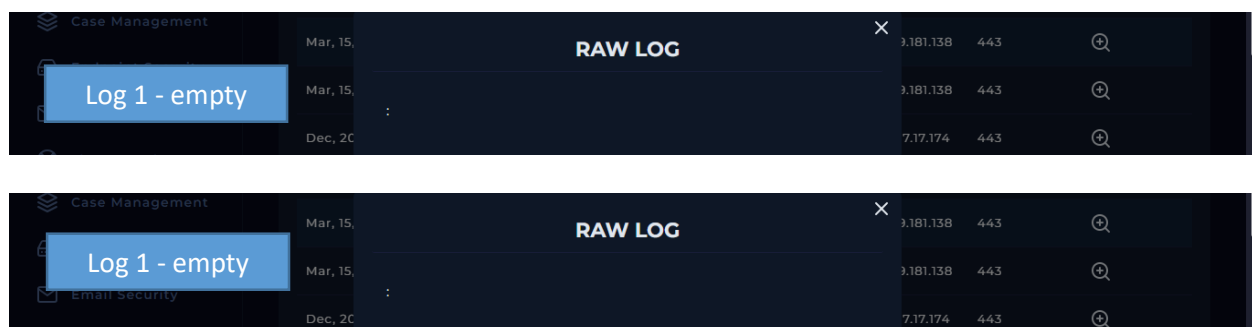
The screenshot shows a 'Log Management' interface with a sidebar menu on the left containing 'Monitoring', 'Log Management', 'Case Management', 'Endpoint Security', 'Email Security', 'Threat Intel', and 'Sandbox'. The main area displays a table of logs with columns: DATE, TYPE, SRC ADDRESS, SRC PORT, DEST. ADDRESS, DEST. PORT, and RAW. A filter is applied to 'Src Address' with the operator 'contains' and the value '172.16.17.55'. The table lists several log entries, including one from 'Mar, 15, 2021, 02:15 PM' and others from 'Dec, 20, 2020'. Two orange arrows point to the 'RAW' column, indicating that the logs have been wiped.

DATE	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
Columns	Operator	Value				
X Src Address	contains	172.16.17.55	1411	120.79.181.138	443	
Mar, 15, 2021, 02:15 PM	Firewall	172.16.17.55	14411	120.79.181.138	443	
Dec, 20, 2020, 05:10 PM	Proxy	172.16.17.55	49283	172.217.17.174	443	
Dec, 20, 2020, 05:11 PM	Proxy	172.16.17.55	47283	172.217.17.174	443	
Dec, 20, 2020, 05:12 PM	Proxy	172.16.17.55	48372	91.198.174.192	443	
Dec, 20, 2020, 05:13 PM	Proxy	172.16.17.55	48273	151.101.1.67	443	
Dec, 20, 2020, 06:23 PM	Proxy	172.16.17.55	49283	151.101.0.81	443	

2 Logs records for the destination IP regarding to our alert date and time.

Both logs have been completely wiped, indicating that the attacker cleared all traces after executing the attack. This suggests a deliberate attempt to cover their tracks and avoid detection, making post-incident analysis and forensic investigation more challenging. “Check the attached photos”.

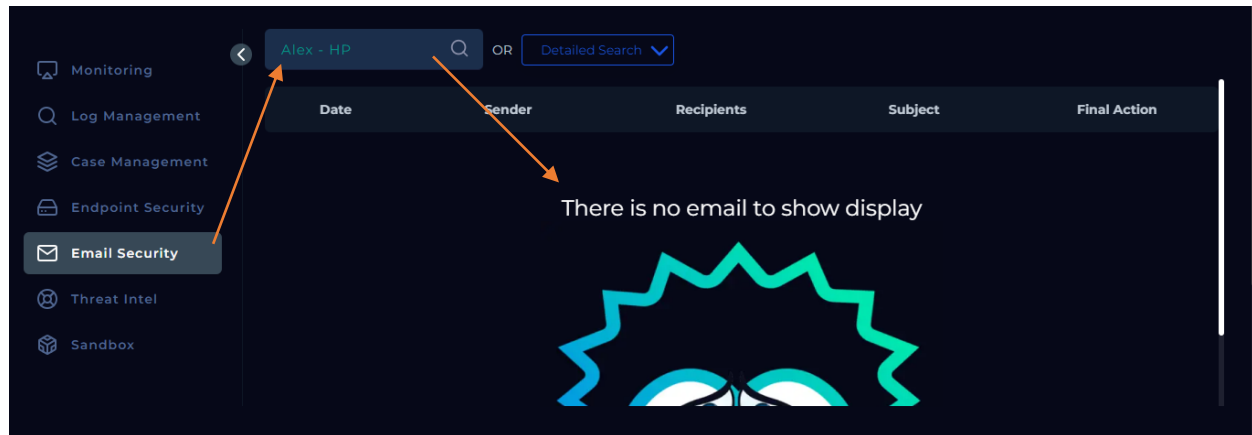
Log Analysis



The two screenshots show 'RAW LOG' windows. The top window has a blue box labeled 'Log 1 - empty' and displays log entries for 'Mar, 15,' and 'Dec, 20'. The bottom window also has a blue box labeled 'Log 1 - empty' and displays log entries for 'Mar, 15,' and 'Dec, 20'. Both windows show a table with columns for DATE, SRC ADDRESS, SRC PORT, DEST. ADDRESS, and DEST. PORT.

DATE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT
Mar, 15,			181.138	443
Mar, 15,			181.138	443
Dec, 20			17.174	443

Email Security:

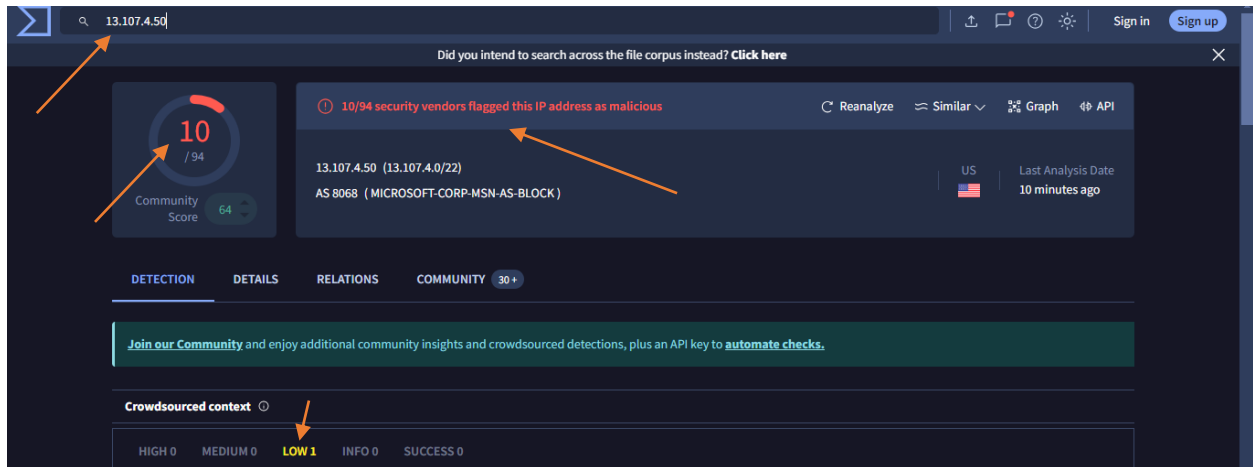


I conducted a thorough check by entering the hostname into the email security system to verify whether the attack was premeditated. The results showed no prior associations or activity, and the email in question was empty. Based on this analysis, there is no indication that the attack was planned in advance, suggesting it was likely opportunistic rather than a targeted campaign.

Detection:

Threat Intelligence Results

We will conduct a comprehensive scan of the Destination IP address using VirusTotal to assess its reputation and determine if it has been associated with any known malicious activities or threats.



VirusTotal Results for Attacker IP: 13.107.4.50

VirusTotal analysis of the source IP address 13.107.4.50 reveals that 10 out of 94 security vendors have flagged this IP as malicious. The detections include the following: •

alphaMountain.ai: Malicious

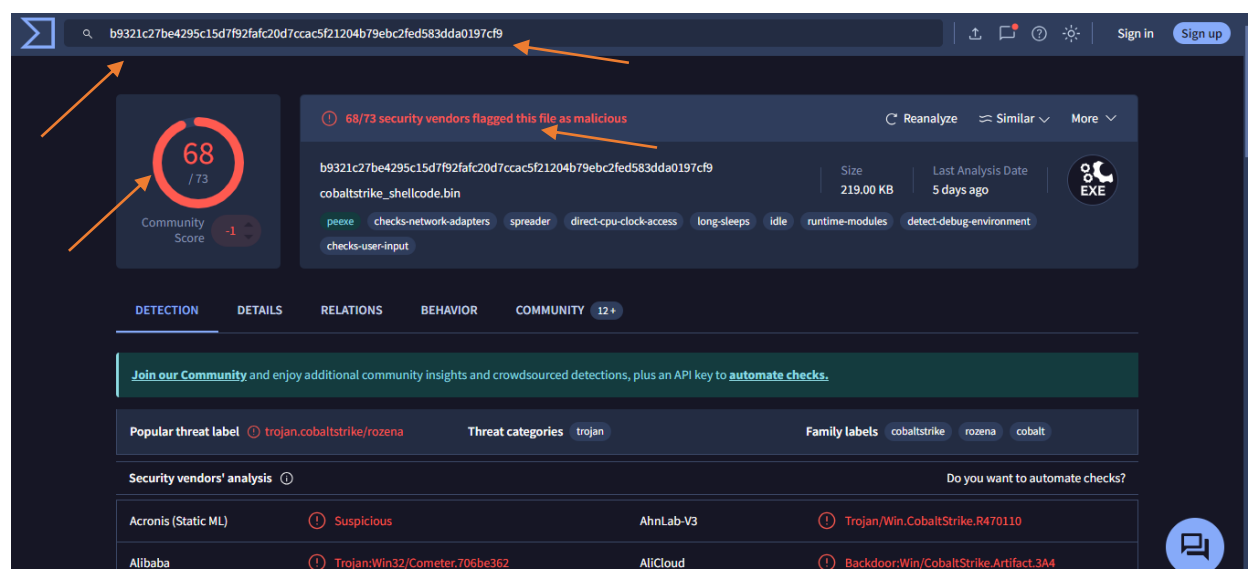
- Antiy-AVL: Malicious
- BitDefender: Malware
- CRDF: Malicious
- CyRadar: Malicious
- ESTsecurity: Malicious
- G-Data: Malware
- Lionix: Malicious
- VIPRE: Malware
- Webroot: Malicious

This indicates a moderate to high level of concern regarding the potential threat posed by this IP address.

Reference result.

- **The Traffic is Malicious**

We will conduct a comprehensive scan File Hash using VirusTotal to assess its reputation and determine if it has been associated with any known malicious activities or threats.



**VirusTotal analysis for the file hash
b9321c27be4295c15d7f92fafc20d7ccac5f21204b79ebc2fed583dda0197cf9**

VirusTotal analysis of the file hash
b9321c27be4295c15d7f92fafc20d7ccac5f21204b79ebc2fed583dda0197cf9 reveals that 68 out of 73 security vendors have flagged this file as malicious. The file is strongly associated with Trojan malware, specifically linked to the CobaltStrike and Rozena families. Notable detections include:

**Threat Labels: **

- Popular threat label: trojan.cobaltstrike/rozena
- Family labels: cobaltstrike, rozena, cobalt

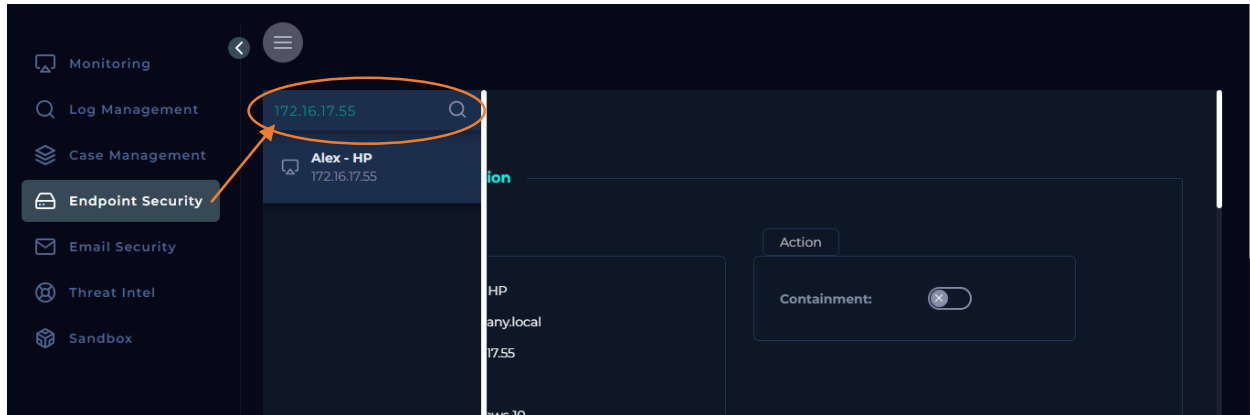
**Security Vendors' Analysis: **

- Acronis (Static ML): Suspicious
- AhnLab-V3: Trojan/Win.CobaltStrike.R470110

- Alibaba: Trojan:Win32/Cometer.706be362
- AliCloud: Backdoor:Win/CobaltStrike.Artifact.3A4
- ALYac: Trojan.CobaltStrike.FM
- Antiy-AVL: GrayWare/Win32.Rozena.wz
- Arcabit: Trojan.CobaltStrike.FM
- Avast: Win32:HacktoolX-gen [Trj]
- AVG: Win32:HacktoolX-gen [Trj]
- Avira (no cloud): TR/Crypt.XPACK.Gen
- BitDefender: Trojan.CobaltStrike.FM
- ClamAV: Win.Backdoor.CobaltStrike-9909816-0
- CrowdStrike Falcon: Win/malicious_confidence_100% (W)
- Cynet: Malicious (score: 100)
- DrWeb: Trojan.Siggen6.51060
- Elastic: Malicious (high confidence)
- Emsisoft: Trojan.CobaltStrike.FM (B)
- ESET-NOD32: Win32/CobaltStrike.Beacon.AE
- Fortinet: W32/Rozena.WZ!tr
- Kaspersky: HEUR:Trojan.Win32.CobaltStrike.gen

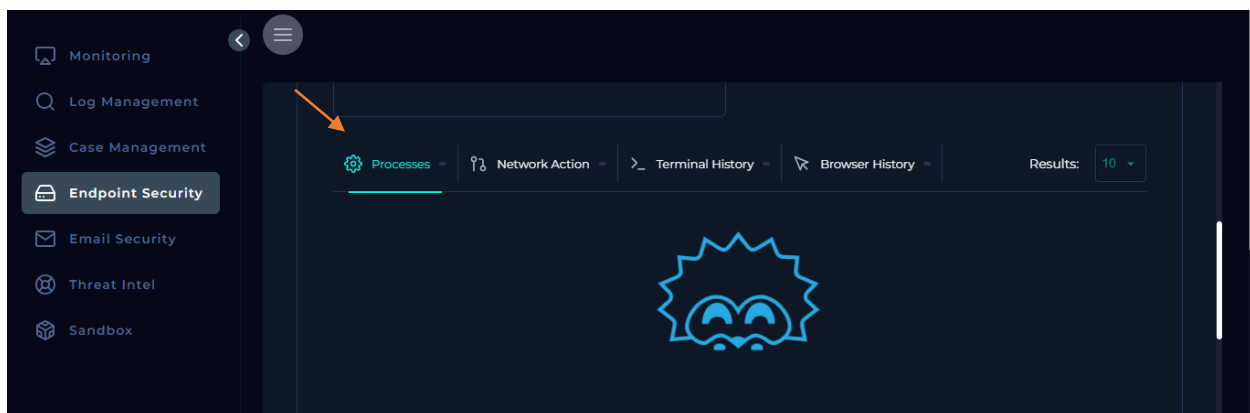
This extensive detection indicates the file poses a significant threat, primarily through its links to the CobaltStrike framework, often used in advanced persistent threats (APTs) for command and control, and Rozena, a backdoor trojan.

Endpoint Security:

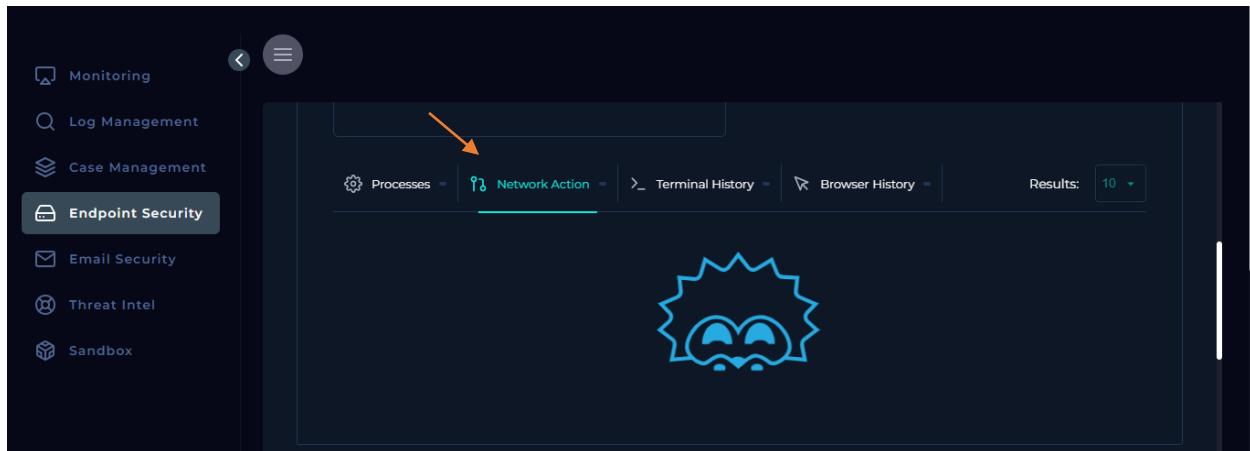


We conducted an analysis of the following sections:

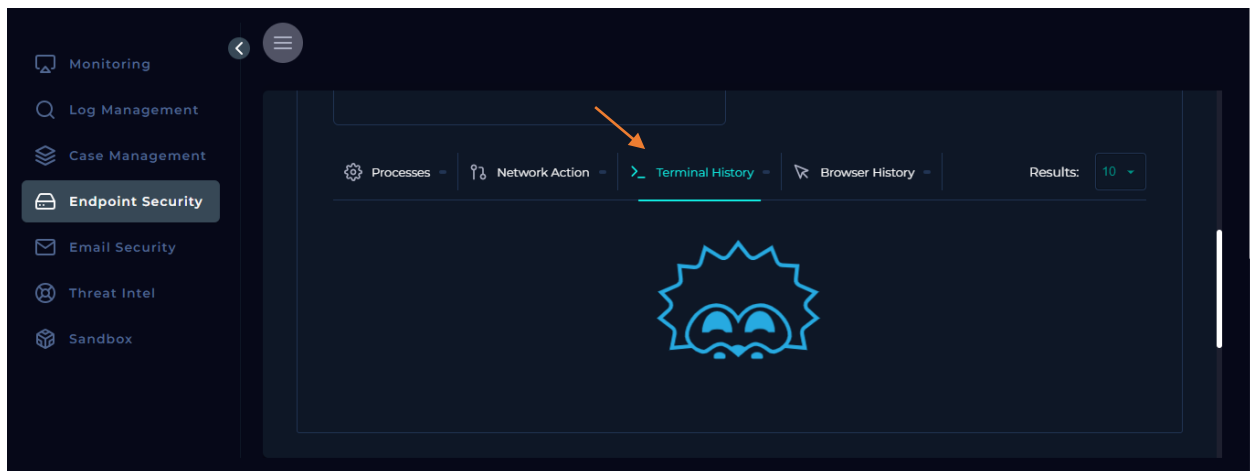
- **Processes section:** No results found. The attacker has successfully cleaned, encrypted, and concealed all data within this section (see attached photo).



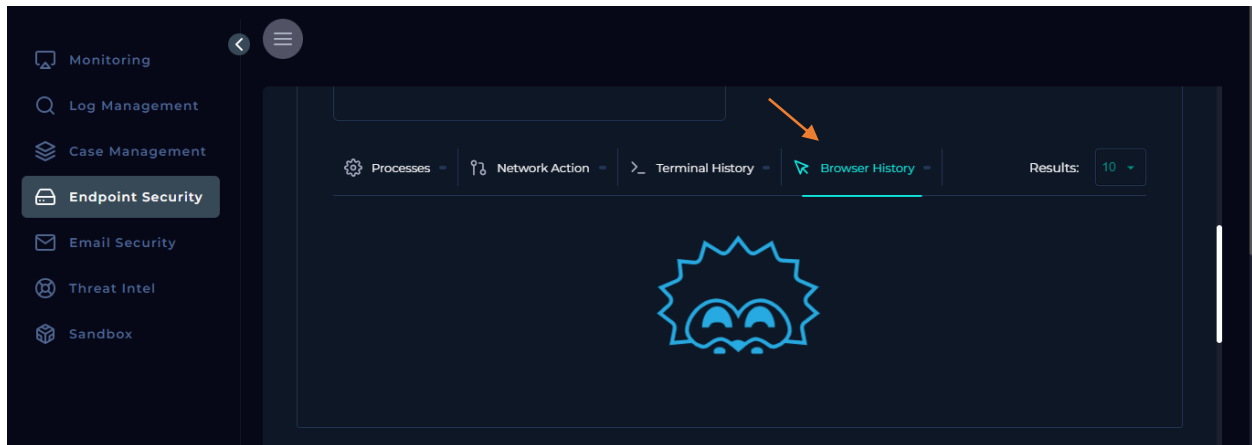
- **Network Action section:** No results found. The attacker has cleaned, encrypted, and hidden all relevant data (see attached photo).



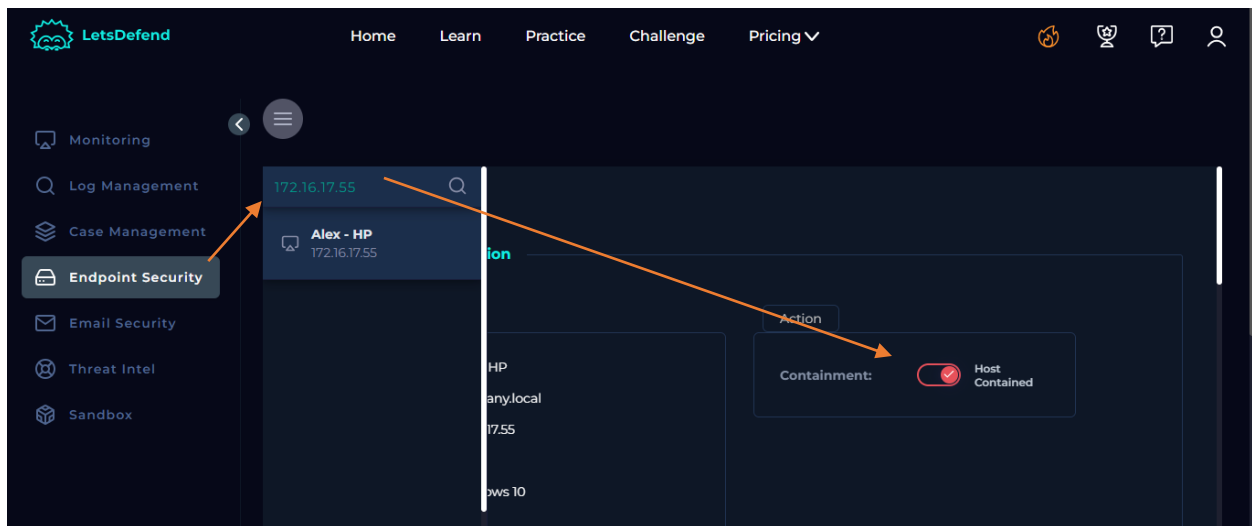
- **Terminal History section:** No results found. The attacker has erased, encrypted, and obscured all data (see attached photo).



- **Browser History section:** No results found. The attacker has removed, encrypted, and hidden all data (see attached photo).



The attacker had full control of the compromised device. Immediate containment is required to prevent further impact.



We have successfully initiated the containment.

Conclusion:

The incident identified on March 15, 2021, at 02:15 PM under Event ID 78 highlights a serious security concern involving Meterpreter or Empire activity, flagged by rule SOC139. This event involved a suspicious executable file named `cobaltstrike_shellcode.exe` that was detected and allowed on the host machine, Alex - HP. The file, with a hash of `24d99ba5654cdf31141c66fd9417b7e0` and a size of 219.00 Kb, displayed clear indicators of malicious intent based on threat intelligence and VirusTotal analysis. This case is particularly concerning due to the attacker's complete control over the compromised device and their ability to clean and conceal crucial forensic data.

The following sections will summarize the key findings of the investigation and highlight the steps required to mitigate future risks.

Attack Overview

Upon detection of the event, a thorough investigation was launched. The attacker's activities were initiated from an internal device with the IP address `172.16.17.55`—part of the organization's internal network. This device attempted to communicate with an external IP address, `13.107.4.50`, a known public IP. While this outbound communication could have been legitimate under different circumstances, the nature of the connection raised suspicion. A VirusTotal scan of the external IP revealed that 10 out of 94 security vendors flagged it as malicious, associating it with known malware families. These detections are indicative of significant risk, suggesting that the attacker was attempting to establish communication with external command and control (C2) infrastructure. The IP address in question is often associated with advanced malware and threat actors, heightening the criticality of this investigation.

Malicious Payload Analysis

The file `cobaltstrike_shellcode.exe` was of particular concern due to its malicious nature. A VirusTotal scan for the file hash showed that 68 out of 73 security vendors flagged the file as malicious. It was associated with the CobaltStrike and Rozena families, known for enabling advanced persistent threats (APTs) by providing attackers with remote access capabilities, lateral movement within the network, and command-and-control functionality. The detections indicated that this file was not a random or benign executable but a highly targeted piece of malware designed to evade detection and execute harmful operations.

The threat labels tied to this file, such as `trojan.cobaltstrike/rozena`, confirm its association with well-established cybercriminal groups. CobaltStrike is commonly used by advanced threat actors for post-exploitation, allowing attackers to establish persistence, move laterally, and escalate privileges within compromised environments. Rozena, a backdoor trojan, further amplifies the risk by providing the attacker with unauthorized remote access to the system, enabling data theft and further malicious activities.

Network and Endpoint Findings

A key focus of the investigation involved assessing network actions and endpoint activities to determine the extent of the attacker's control over the compromised system. Despite rigorous efforts to analyze the following sections—Processes, Network Action, Terminal History, and Browser History—no meaningful results were obtained. It became evident that the attacker had successfully cleaned, encrypted, and hidden all relevant data, a sophisticated tactic employed by advanced threat actors to cover their tracks. By erasing logs and concealing activities across multiple critical sections, the attacker effectively hindered the incident response team's ability to trace and understand the full scope of the attack.

The complete erasure of logs in these key sections points to a highly skilled adversary with the knowledge and resources to manipulate endpoint data. The attacker's actions suggest that they gained full control of the compromised device, potentially allowing them to execute any number of malicious actions undetected. These could range from data exfiltration and lateral movement to the installation of additional backdoors, all of which pose severe risks to the organization's security posture.

Threat Intelligence and Contextual Analysis

In terms of broader threat intelligence, the IP address `13.107.4.50` was identified as malicious by 10 reputable security vendors, including BitDefender, VIPRE, and Webroot. These detections classified the IP address as part of a broader infrastructure used by cybercriminals to launch attacks, particularly involving trojans and remote access tools (RATs). Given the strong correlation between the file `cobaltstrike_shellcode.exe` and this IP, it is likely that the attacker was leveraging a known threat infrastructure for their activities. This further underscores the need for swift containment and remediation to prevent any further exploitation.

The VirusTotal results also reveal the advanced nature of the malware used in this attack. CobaltStrike, often used in penetration testing, has become a popular tool among cybercriminals due to its ability to mimic legitimate system administration tasks while performing malicious activities. Its use in this incident signals a well-planned attack that leverages sophisticated tools to avoid detection and maintain persistence within the network.

Email Security Review

A comprehensive review of the email security system was also conducted to determine if this attack was premeditated or opportunistic. By checking the hostname `Alex - HP` against the email security logs, no prior associations or activity were found. The email itself was empty, indicating that this attack was likely not part of a coordinated phishing campaign or planned intrusion. Instead, the attacker may have exploited a vulnerability or leveraged stolen credentials to gain initial access to the network. This opportunistic nature further emphasizes the importance of proactive monitoring and threat detection to identify and mitigate potential vulnerabilities before they can be exploited.

Containment and Recommendations

Given the severity of the attack, immediate containment measures were initiated, including isolating the compromised device and preventing further communication with external IPs. This action was critical to halting any ongoing malicious activity and minimizing potential damage. However, the sophistication of the attacker, particularly their ability to wipe logs and conceal activities, indicates that further steps are necessary to fully secure the environment.

Moving forward, I recommend the following actions:

1. **Forensic Investigation**: Engage in a deeper forensic analysis of the compromised system to uncover any residual traces of the attacker's activities. This may involve memory analysis, file system examination, and a review of any remaining artifacts.
2. **Network Segmentation**: Strengthen network segmentation to limit the movement of attackers within the environment. This will reduce the likelihood of lateral movement in the event of future compromises.
3. **Enhanced Monitoring**: Implement advanced threat detection systems that focus on behavioral analysis and anomaly detection to identify similar attacks in the future. This should include monitoring outbound traffic for unusual patterns that may indicate command-and-control activity.
4. **Patch Management**: Review and update all security patches across the environment, with particular attention to vulnerabilities that may have been exploited in this incident.
5. **Incident Response Readiness**: Ensure that the incident response team is well-prepared to handle future attacks by conducting regular tabletop exercises and refining response playbooks.

Conclusion

This incident serves as a stark reminder of the evolving nature of cyber threats and the importance of maintaining a proactive and layered defense strategy. The attacker's use of advanced tools like CobaltStrike and their ability to evade detection highlights the need for constant vigilance and improved detection mechanisms. By promptly containing the threat and initiating remediation efforts, we have minimized the immediate impact of the attack. However, it is imperative that we continue to strengthen our defenses to prevent future incidents and stay ahead of increasingly sophisticated adversaries.

In conclusion, the success of this investigation demonstrates our team's ability to respond to advanced threats effectively. Despite the attacker's attempts to cover their tracks, we were able to analyze the situation comprehensively and take decisive action to contain the threat. This report underscores the critical importance of ongoing threat intelligence, advanced monitoring, and a well-prepared incident response team in safeguarding our organization against future attacks.